UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/808,973	03/24/2004	Ned M. Smith	42P18125	7029

59796 7590 09/13/2007

INTEL CORPORATION
c/o INTELLEVATE, LLC
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER	
TRAORE, FATOUMATA	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
09/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/808,973	SMITH, NED M.	
	Examiner	Art Unit	
	Fatoumata Traore	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15 and 33-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15 and 33-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response of the restriction/election requirement filing on August 10th, 2007. Applicant without traverse withdraws claims 16-32. Therefore, claims 1-15 and 33-47 are pending.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 33-47 are drawn to a computer readable medium, which the applicant has defined in the specification (page 34, paragraph [0105]) to encompass an electronic transmission signal (carrier wave). The Office considers an electronic signal to be a form of energy. Energy is not a series of steps or acts and this is not a process. Energy is not a physical article or object and as such is not a machine or manufacture. Energy is not a combination of substances and therefore not a compilation of matter. Thus, an electronic transmission signal does not fall within any of the four categories of invention.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent

granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-6, 12, 13, 15, 33—38, 44, 45, 47 are rejected under 35 U.S.C. 102(e) as being anticipated by **Uusitalo et al** (US 2005/0063544).

Claims 1, 33: **Uusitalo et al** discloses a method and article of facilitating the lawful interception of an IP session between two or more terminals comprising:

a. Simultaneously authenticating multiple facets of an endpoint (key exchange procedure between the terminals) (paragraphs [0007] , [0010], [0017], [0018]; and Fig. 7);

b. Combining the multiple facets of the endpoint with a pre-master secret (the parties involved in the session to agree upon a Pre-Master Key (PMK) for use in securing traffic sent over the session) (paragraphs [0008], [0012]);

c. Cryptographically hashing a platform configuration (for security reasons secret key (k) may not be used directly to encrypt traffic, but rather some traffic encryption key (TEK) is derived from the PMK k (e.g. by taking a hash of the PMK) (paragraph [0048]);

d. Mixing the cryptographically hashed platform configuration with the pre-master secret via hash to generate a master secret (paragraph [0049]); and

e. Encrypting the master secret to authenticate a negotiated channel the Multi-Media key management function may encrypt the PMK with a secret key which it shares with the responder, or with the public key of the responder, or the

initiator may calculate a Diffie-Hellman modular exponentiation to obtain the PMK) (paragraph [0007]

Claims 2, 34: **Uusitalo et al** discloses a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 1 and 33 above, and further discloses that the platform private key is bound to the platform configuration using a trusted platform device when a subscriber registers with the operator of a 3GPP network, he or she receives a Subscriber identity Module (SIM) card on which is stored a unique International Mobile Subscriber Identity (IMSI) code (paragraph [0032]).

Claims 3, 35: **Uusitalo et al** discloses a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 2 and 34 above, and further discloses that the trusted platform device comprises a processor coupled to a protected storage device (paragraph [0053]; Fig .7).

Claims 4, 36: **Uusitalo et al** discloses a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 1 and 33 above, and further discloses a step of cryptographically hashing the platform configuration comprises cryptographically hashing the platform configuration using a secure hashing algorithm (a pseudo-random function such as a keyed hash (or MAC, Message authentication code) such as SHA-1 or MD5 or the 3GPP Milenage algorithm)(paragraph [0032]).

Claims 5, 37: **Uusitalo et al** discloses a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 4 and 36

above, and further discloses that the secure hashing algorithm comprises Secure Hashing Algorithm Version 1.0 (SHA-1) (paragraph [0032]).

Claims 6, 38: **Uusitalo et al** discloses a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 1 and 33 above, and further discloses that the step of encrypting the master secret comprises digitally signing the master secret with one or more certified keys (traffic encryption key is derived from either by means of a previously known shared secret key, or by digital signatures and certificates) (paragraph [0048]).

Claims 12, 44: **Uusitalo et al** discloses a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 1 and 33 above, and further discloses a step of enabling the encrypted master secret to be decrypted at another endpoint, wherein the master secret is used by each endpoint to generate the session keys (paragraphs [0013], [0036], [0050]).

Claims 13, 45: **Uusitalo et al** discloses a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 1 and 33 above, and further comprises:

a. Exchanging an explanation of the platform configuration hashes following session key negotiations to finalize the authentication (paragraph [0032]);

b. Verifying, at both endpoints, key exchange messages, certificates and platform configuration data (paragraphs [0053], [0088]); and

c. Authenticating the session if no problems arise during verification (paragraphs [0053], [0054]).

Claims 15, 47: **Uusitalo et al** discloses a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 13 and 45 above, and further discloses a step of enabling endpoints to exchange data, wherein each endpoint knows that the platform from the other endpoint has been authenticated using a platform identity that ties to the trusted platform module (paragraph [0032]).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims7-9, 10-11, 39-41, 42-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Uusitalo et al** (US 2005/0063544) in view of **Morgan et al** (US 20020184491).

Claims 7-9, 39-41: **Uusitalo et al** discloses a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 6 and 38 above, but does not explicitly discloses that one or more certified keys includes a user key and a platform key. However, **Morgan et al** discloses a method and article of authentication to support secure data transfer, which further discloses that one or more certified keys includes a user key and a platform key (paragraphs [0015], [0019]). Therefore, it would have been obvious for one having ordinary skills in the art at the

time the invention was made to include a platform key and a user key. One would have been motivated to do so in order to prevent unauthorized access to critical data.

Claims 10-11, 42-43: **Uusitalo et al** discloses a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 6 and 38 above, but does not explicitly discloses that the platform configuration includes multiple identities and one or more certified keys includes one or more platform identity keys. However, **Morgan et al** discloses a method and article of authentication to support secure data transfer, which further discloses that the platform configuration includes multiple identities and one or more certified keys includes one or more platform identity keys (paragraph [0019]). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made to include a platform key and a user key. One would have been motivated to do so in order to prevent unauthorized access to critical data.

7. Claims 14, 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Uusitalo et al** (US 2005/0063544) in view of **Bass et al** (US 4649233).

Claims 14, 46: **Uusitalo et al** discloses a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 13 and 45 above, but does not explicitly discloses a step of halting the authentication. However, Bass et al discloses a method and article to support secure data transfer, which further discloses a step of halting the authentication session if problems arise during verification (column 4, lines 35-51). Therefore, it would have been obvious for one

having ordinary skills in the art at the time the invention was made to include a a step of halting the authentication. One would have been motivated to do so in order to prevent unauthorized access to critical data.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Monday, September 10, 2007

Nassar G. Moazzami
Supervisory Patent Examiner

9/11/07